資料3－3

SIMカードへの利用者認証機能の格納実現に向けた技術的な検討課題の詳細化について

2016年2月16日

大日本印刷株式会社
情報ソリューション事業部
事業企画本部
社会情報基盤プロジェクトチーム

DNP

技術的な検討課題の詳細化　1

稼働中の民間スキームであるモバイルNFCサービス（クレジット）等での実績を参考に、
第2回SWG「資料２－３」で提示された技術的な検討課題の詳細化について、検討を行いました。

（DNP追記は、青網掛け部）

1．技術的な検討課題		検討課題の詳細化（案）	参照基準（案）
（１）電子証明書及び秘密鍵のSIMカードへダウンロード	ア．SIMカードの電子証明書等の格納媒体としての要件（セキュリティの確保）	① 対象とするSIMカード（現行品、新規開発品） ② 機能要件（暗号アルゴリズム、メモリ容量、SIM内での鍵ペア生成、アプレット及びパーソナライズデータのセキュアダウンロード） ③ アプレット開発（SIM毎のカスタマイズ要否（速度等の機能要件等への対応）） ④ 認定要件　（J-LIS様） ・認定単位　（JPKIアプレットとSIMを一体で認定？） ・認定効率化（国際クレジット認定結果の参照　等） ・参照基準（案）（右記）の適用範囲（現行品、新規開発品）	「通知カード及び個人番号カードに関する技術的基準」 「認証業務及びこれに附帯する業務の実施に関する技術的基準」 等
	イ．SIMカードへの電子証明書等の安全なダウンロードの方法（ネットワーク経由又は窓口における格納）	① SIMカードへのアプレットダウンロード（ダウンロード関連鍵の格納場所、ダウンロード方法＝新規開発品に統一要否） ② パーソナライズ（証明書ダウンロード）データと対象SIMとの対応付け方法（SP-TSMが利用できるSIM個別情報の要否等） ③ SIM仕様差分の許容範囲 ・アプレットダウンロード仕様等、SIMの仕様差分（MNO、Ver.）の許容可否（許容する場合、MNO-TSMで差分対応） ・パーソナライズ（証明書ダウンロード）時に、SIMの仕様差分の許容可否（許容する場合、SP-TSMで差分対応） ④ 証明書有効期限到来時の対応方法	

<参考1>開発・認定要件の比較
<参考2>全銀協ICキャッシュカード認定制度の例　参照

技術的な検討課題の詳細化　2

（DNP追記は、青網掛け部）

1．技術的な検討課題		検討課題の詳細化（案）	参照基準（案）
	ウ．スマートフォンの要件	①対象機種 ・〇NFCスマホ（android）※　※非MNO提供端末は、別途確認要 ・×iPhone（アップル以外の他社に仕様開示されていない） ・△非NFCスマホ（android）・・・TSMとの通信機能プリセット有無 ②機能要件 ・ダウンロード時の書き込みI/F（携帯電話網、Wi-Fi） ・NFCスマホ限定となる要件の有無確認 ・TSMとの通信機能（仕様差分の許容範囲） ③UIアプリの開発、検証 （対象機種、OS Ver.、検証用NFCリーダ） ④新機種検証（実施主体、検証基準）	
（２）既存システムへの影響	ア．JLISのJPKIシステムの改修（スマートフォンにダウンロードされた電子証明書の発行・管理機能（個人番号カードの電子証明書との紐付け、有効期限等ライフサイクル管理（発行、失効、一時停止）））	①個人番号カード紛失時の取り扱い（スマホ証明書の有効性）	

<参考1> 開発・認定要件の比較

稼働中のICカードスキーム(①②)を参考に、モバイルNFC(JPKI)の場合(③)の開発・認定要件(案)の検討を行いました。

	①モバイルNFC(クレジット) (非接触クレジット機能をSIMに搭載)		②全銀ICキャッシュ(クレジット一体型) (複数アプリ(ICキャッシュ、クレジット)を搭載したICカードの例)(<参考2>参照)		③モバイルNFC(JPKI)(案) (利用者証明機能をSIMに搭載)	
	開 発	認 定	開 発	認 定	開 発	認 定
SIM (ICカード)	SIMベンダ	SIM+アプレット 一体での認定 クレジット国際ブランド (機能、セキュリティ) 及び GlobalPlatform (ダウンロード)	ICカードベンダ	ICカード+アプレット 一体での認定 クレジット国際ブランド (機能、セキュリティ) ↓ ICキャッシュカード認定 制度運営協議会 (ICTAC) ※2 (機能(ICキャッシュ))	SIMベンダ	SIM+アプレット 一体での認定 クレジット国際ブランド (機能、セキュリティ) 及び GlobalPlatform (ダウンロード) 現行SIM(①)での認定取得範囲 ↓ J-LIS認定 (機能、セキュリティ) ・JPKIアプレットのインストール ・パーソナライズ(証明書等の書込) ・JPKI利用者証明機能の利用 ・ライフサイクル管理 ・NFC通信試験(リファレンス端末にて実施)
アプレット	VISA=VISAより提供 Master=SIMベンダで開発		ICカードベンダ		SIMベンダ or J-LIS	
UIアプリ	SP (サービス提供事業者)	クレジット国際ブランド	なし	なし	J-LIS	
SP-TSM	SP	PCI DSS ※1 及び クレジット国際ブランド (プライバシーマーク、 ISO9001、ISMS)	なし	なし PCI DSSの要件(SP-TSM関連) ●安全なネットワークの構築と維持 ●会員データを保護管理するプログラムの整備 ●脆弱性を管理するプログラムの整備 ●強固なアクセス手法の導入 ●定期的なネットワークの監視とテスト ●情報セキュリティポリシーの整備 ●定期的な作業手順の検証 ●セキュリティ監査への適合	SP	
端末	端末ベンダ (スマートフォン)	EMVCo.	端末ベンダ (ATM)	EMVCo. ICTAC ※2	端末ベンダ (スマートフォン)	

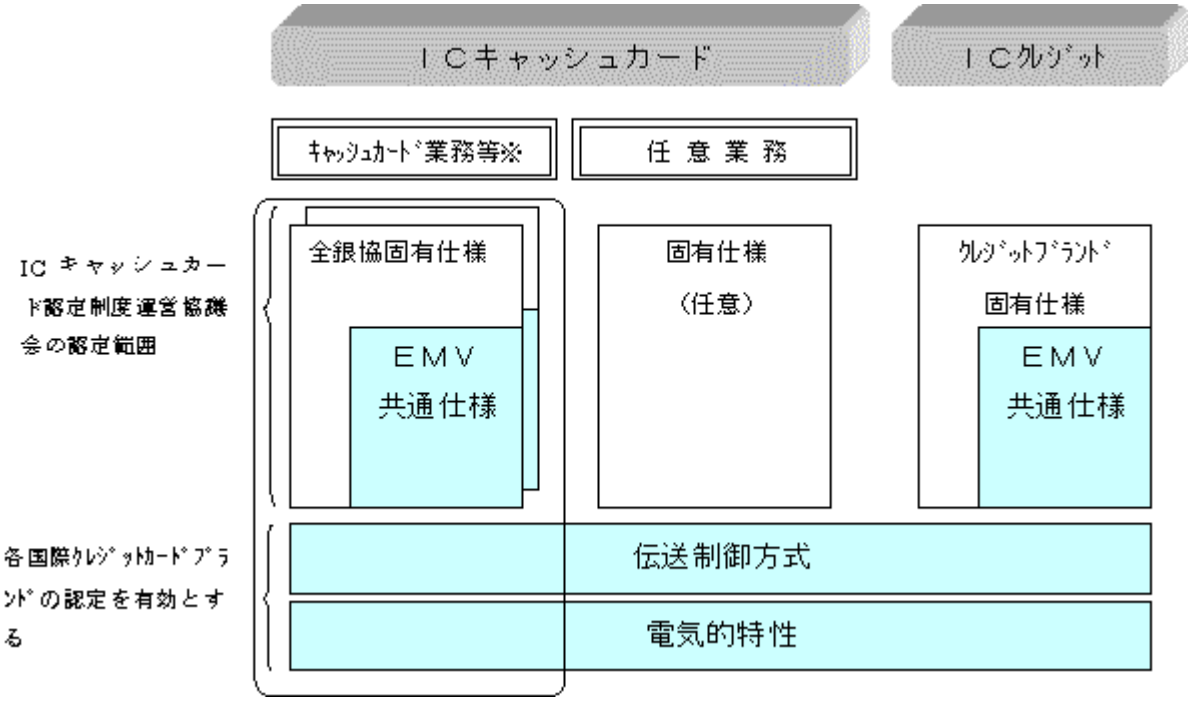
※1 PCI DSS(Payment Card Industry Data Security Standards):加盟店やサービスプロバイダ等でクレジットカードの会員データを安全に取り扱うことを目的に策定されたクレジットカード業界の国際的なセキュリティ基準。国際カードブランド5社が共同設立したPCI SSC(Security Standards Council)が運用、管理している。

※2 電気的特性、伝送制御等の共通部分は、クレジット認定結果を参照

＜参考2＞ 全銀協ICキャッシュカード認定制度の例

ICキャッシュカード認定制度運営協議会　ホームページより
http://www.ictac.jp/kaisetsu2.htm

■ **EMV仕様におけるICカードの認定は、現状、各国際クレジットカードブランドにおいて実施されていることから、EMVCo.といった統一された認定制度は存在せず、認定のための試験内容についても公表されていません。**
**　そのため、カードの伝送制御方式および電気的特性については、<u>各国際クレジットブランドの認定を有効としつつ</u>、アプリケーション部分については、EMV仕様をベースに、標準仕様にもとづいた<u>協議会独自の試験項目を定めています</u>。**



DNPは、NFCフォーラムのスポンサー会員です。

大日本印刷株式会社

情報ソリューション事業部
事業企画本部
社会情報基盤プロジェクトチーム